***Dr Artur Romaszewski***
*Uniwersytet Jagielloński - Collegium Medicum*
*Wydział Nauk o Zdrowiu*
*Zakład Medycznych Systemów Informacyjnych*
*artur.romaszewski@uj.edu.pl*

***Dr hab. med. Wojciech Trąbka***
*Uniwersytet Jagielloński - Collegium Medicum*
*Wydział Nauk o Zdrowiu*
*Zakład Medycznych Systemów Informacyjnych*
*wojciech.trabka@uj.edu.pl*

***Mgr Mariusz Kielar***
*Uniwersytet Jagielloński - Collegium Medicum*
*Wydział Nauk o Zdrowiu*
*Zakład Medycznych Systemów Informacyjnych*
*mariusz.kielar@uj.edu.pl*

***Mgr Krzysztof Gajda***
*Uniwersytet Jagielloński - Collegium Medicum*
*Wydział Nauk o Zdrowiu*
*Zakład Medycznych Systemów Informacyjnych*
*krzysztof.gajda@uj.edu.pl*

# WPROWADZENIE USŁUG ZAUFANIA ZGODNYCH Z ROZPORZĄDZENIEM UE eIDAS W ASPEKCIE SYSTEMÓW INFORMACYJNYCH OPIEKI ZDROWOTNEJ (CZĘŚĆ I)

## Wstęp

Czas wprowadzenia usług zaufania uregulowanych w rozporządzeniu eIDAS, będących tematem tego artykułu, to 1 lipca 2016 roku. Powyższa data staje się tym samym wyraźną cezurą czasową rozpoczynającą implementację systemu usług zaufania. Biorąc pod uwagę szereg zaprezentowanych w artykule problemów praktycznych i zmian wprowadzanych na mocy wchodzących w życie przepisów unijnych, istotną kwestią z punktu widzenia ich konsekwencji prawnych wydaje się już być sama forma rozporządzenia (nie dyrektywy) nadana eIDAS przez ustawodawcę. Rozporządzenie Unii Europejskiej jest bowiem aktem prawnym zasadniczo różniącym się od dyrektywy. O ile dyrektywa unijna podlega implementacji przez kraje członkowskie w systemie prawa krajowego, o tyle przepisy rozporządzenia są

bezpośrednio stosowane w krajowym porządku prawnym. Skutek rozporządzenia nie zależy przy tym od krajowych środków implementujących w jakikolwiek sposób, czy też wprowadzających, rozporządzenie do krajowego porządku prawnego. Dla mocy obowiązującej rozporządzenia nie jest konieczny akt inkorporacji jego przepisów do prawa krajowego[1].

Forma rozporządzenia wyklucza możliwość korygowania tych przepisów przez państwa członkowskie. Państwo członkowskie ma jednak prawo doprecyzowania, czy dookreślania tych obszarów, które prawodawca unijny pozostawił niedookreślone, lub wprost odesłał do prawa krajowego,. Możliwe jest zatem doprecyzowanie obszarów, które w rozporządzeniu elDAS pozostały "otwarte", ale pod warunkiem, że sposób tego doprecyzowania nie będzie stał na przeszkodzie osiągnięciu celów rozporządzenia[2]. W Polsce trwa proces przygotowywania aktów prawnych mających za zadanie uregulowanie zagadnień nie uregulowanych na poziomie rozporządzenia eIDAS. Należy określić skutki prawne dla usług zaufania, które nie zostały określone w rozporządzeniu eIDAS. Opracować należy również zasady i przesłanki odpowiedzialności cywilnoprawnej podmiotów świadczących usługi zaufania, oraz sposoby i środki nadzoru, monitoringu i kontroli podmiotów świadczących usługi zaufania. Ustawa winna regulować zasady funkcjonowania rynku usług zaufania określając warunki rozpoczęcia i zakończenia działalności kwalifikowanych usługodawców, jak też warunki zawieszenia certyfikatów[3].

Będzie to miało szczególne znaczenie dla systemów administracji publicznej naszego kraju, w tym dla systemów informacyjnych opieki zdrowotnej. W sektorze zdrowia nadal niedokończone i nie w pełni funkcjonalne pozostają platformy teleinformatyczne zaprojektowane w ramach Systemu Informacji Medycznej. Dlatego sprawne przyjęcie zróżnicowanego modelu usług zaufania wymaganych przez eIDAS może w praktyce napotkać na liczne bariery, związane przede wszystkim z głębokim niedostosowaniem infrastruktury informacyjnej naszego państwa do przedmiotowych regulacji.

W artykule omówiono ideę otwartych i zamkniętych usług zaufania oraz ich rodzaje. Przedstawiono koncepcję krajowej infrastruktury zaufania oraz narodowego centrum

[1] Wróbel A., [w]: *Traktat o funkcjonowaniu Unii Europejskiej*. Komentarz. Tom III pod red. D. Kornobis-Romanowskiej i J. Łacny, Warszawa 2012
[2] Mielnicki T. Wołowski F., Grajek M., Popis P. Łuczak P., Tabor M., Brakoniecki M., *Identyfikacja i uwierzytelnienie w usługach elektronicznych*, Forum Technologii Bankowych przy Związku Banków Polskich, Warszawa 2013
[3] Tamże

certyfikacji usług zaufania. Rozporządzenie eIDAS, między innymi, wprowadza zmiany w istniejących usługach jak np. podpis elektroniczny. Wprowadza również nowe usługi jak pieczęć elektroniczna, uwierzytelnienie witryn internetowych oraz konserwacja elektronicznych podpisów, pieczęci i certyfikatów.

## Usługi zaufania

Obecnie trwają pracę nad przepisami mającymi za zadanie umożliwienie wejścia w życie usług zaufania[4]. Rozporządzenie elDAS odsyła do prawa krajowego w zakresie zasad odpowiedzialności cywilnoprawnej dostawców usług zaufania. Prawo krajowe musi zapewnić wprowadzenie do obrotu prawnego nowych usług zaufania. Do zmiany jest siatka pojęciowa funkcjonująca dotychczas w wielu aktach prawnych w Polsce. W tym celu należy dodać nowe pojęcia i wyeliminować pojęcia oraz instytucje nieznane w rozporządzeniu elDAS np. bezpieczny podpis elektroniczny (Rysunek 1).

Usługa zaufania oznacza usługę elektroniczną, zazwyczaj świadczoną za wynagrodzeniem obejmującą:

- tworzenie, weryfikację i walidację podpisów elektronicznych, pieczęci elektronicznych lub elektronicznych znaczników czasu, usług rejestrowanego doręczenia elektronicznego oraz certyfikatów powiązanych z tymi usługami;
- tworzenie, weryfikację i walidację certyfikatów uwierzytelniania witryn internetowych;
- konserwację elektronicznych podpisów, pieczęci lub certyfikatów powiązanych z tymi usługami.[5]

## Otwarte i zamknięte usługi zaufania

[4] Projekt ustawy o usługach zaufania oraz identyfikacji elektronicznej z 03.06.2016 r. - https://legislacja.rcl.gov.pl/projekt/12283556

[5] Art. 3 ust. 16 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr. 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE

Usługi zaufania można podzielić na:

- otwarte usługi zaufania – są to usługi, które oznaczają zestaw usług zaufania świadczonych na rzecz społeczeństwa mające skutki dla stron trzecich.
- zamknięte usługi zaufania – oznaczają zestaw usług zaufania świadczonych na rzecz określonej, dobrze zdefiniowanej grupy użytkowników i nie mających skutków dla stron trzecich. Są usługami świadczonymi poza nadzorem i działaniem rozporządzenia eIDAS.
  Jego przepisy nie mają zastosowania do świadczenia usług zaufania wykorzystywanych wyłącznie w obrębie zamkniętych systemów wynikających z prawa krajowego lub z porozumień zawartych przez określoną grupę uczestników (zob. art. 2 ust. 2 rozporządzenia elDAS).

Przedstawiony podział usług ma na tyle istotne znaczenie, że pozwala na określenie granicy pomiędzy usługami zaufanymi, podlegającymi nadzorowi i wymaganiom rozporządzenia eIDAS oraz usługami, które powyższym wymogom nie podlegają (usługi zamknięte)[6]. Podział na usługi otwarte i zamknięte ma istotne znaczenie dla systemów informacyjnych funkcjonujących w ochronie zdrowia. Dotyczy to zarówno systemów planowanych na szczeblu ogólnokrajowym, jak systemów już funkcjonujących w szpitalach i poradniach w lecznictwie otwartym.

Usługi świadczone w ramach systemu zamkniętego będą dużo tańsze, niż usługi, dla których trzeba zastosować szereg wymaganych prawem procedur i standardów. Nie zawsze prosta analiza umożliwia wskazanie, z którą grupą usług mamy do czynienia. Poniżej zamieszczono przykłady możliwych sytuacji praktycznych.

Gmina świadczy usługi zaufania na rzecz mieszkańców gminy wydając im certyfikaty. Za pomocą tych certyfikatów mieszkańcy zapewniają autentyczność pism wysyłanych do gminy. W oparciu o te pisma urzędnicy gminy podejmują decyzje, które mogą mieć wpływ na strony trzecie np. spadkobierców mieszkających poza gminą. Łatwo zauważyć, że mieszkańców można uznać za zamkniętą grupę, ale skutki świadczenia usług zaufania wykraczają poza członków tej grupy[7].

[6] Stanowisko Poczty Polskiej
https://legislacja.rcl.gov.pl/docs//2/12283556/12343437/12343440/dokument216770.pdf
[7] Pejaś J., Szulga M.,Wagemann M., Stoliarowa-Myć A., Wiktorczyk P., Wdrożenie rozporządzenia elDAS w Polsce – raport, http://www.internet.pl/wp-content/uploads/2014/07/Ekspertyza-Główna-w.-4-2.pdf

Jeżeli szpital wydaje certyfikaty swoim pacjentom, to stanowią oni otwartą grupę, ponieważ każdy może skorzystać z usług szpitala . W tym przypadku grupa pacjentów jest grupą otwartą gdyż każdy ma prawo założyć konto w szpitalu i korzystać z jego systemu, a skutki przynależności wykraczają poza tę grupę (np. skutki niezgodnego z prawem uzyskania danych, będące efektem wykorzystania usługi zaufania, mogą dotyczyć zarówno pacjentów, jak również podmiotów spoza tej grupy).

Systemem zamkniętym będzie natomiast system pracowników administracji szpitala służący do obsługi wewnętrznych dokumentów tworzonych i akceptowanych przez urzędników różnych komórek organizacyjnych.

W przewidywanych w 2015 roku propozycjach zmian w ustawie o systemie informacji w ochronie zdrowia oraz innych ustaw wynikało, że w ramach infrastruktury PKI NFZ (infrastruktura klucza publicznego) wydawane będą certyfikaty kwalifikowane i niekwalifikowane. Certyfikaty te miały być instalowane na kartach eKUZ, KSM (karta specjalisty medycznego) i KSA (karta specjalisty administracyjnego). Czy można zatem przyjąć, że kwalifikowane usługi zaufania świadczone przez PKI NFZ są zamkniętymi usługami? Z rozważań wynika, że tego typu usługi są usługami otwartymi i tym samym podlegają wymaganiom określonym w rozporządzeniu eIDAS. Ponadto należy przyjąć (założyć), że usługi te powinny być świadczone za pośrednictwem firm, które będą działały na zasadach rynkowych (zasada ta powinna dotyczyć także usług niekwalifikowanych w przypadku, gdy PKI NFZ nie świadczy ich jedynie na potrzeby własne)[8].

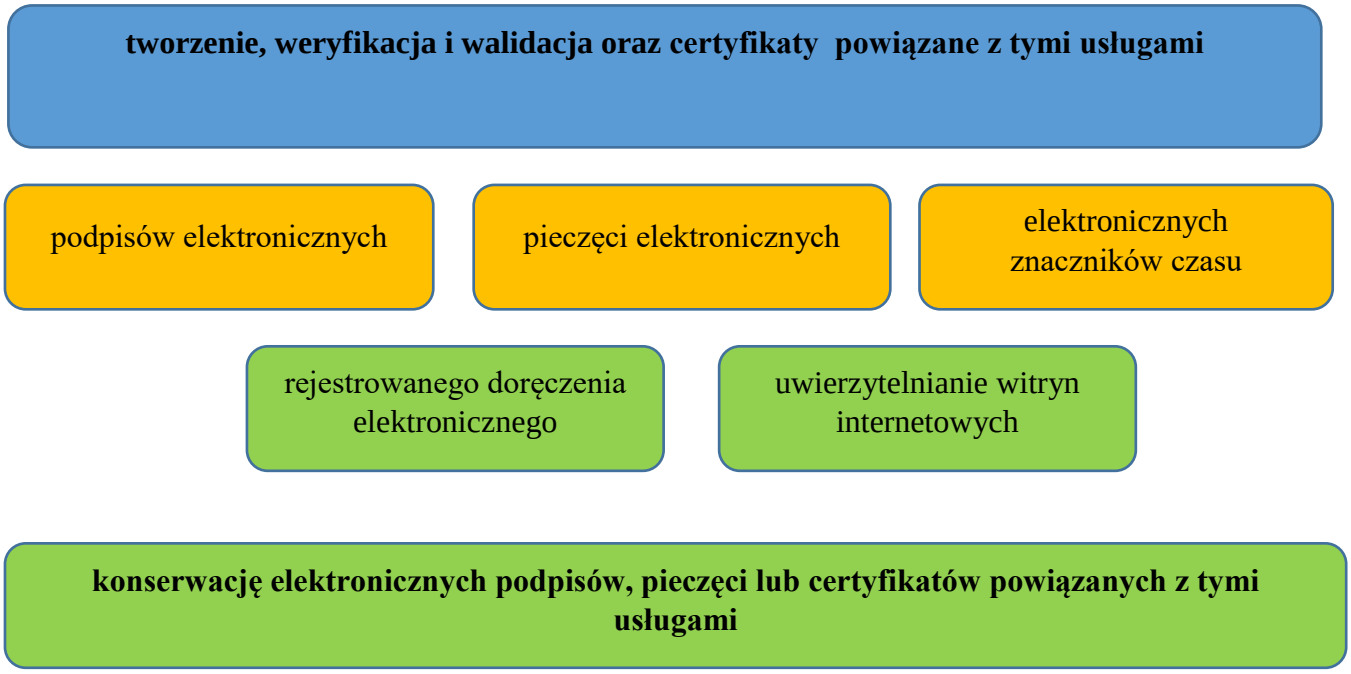
Rozporządzenie wprowadza ogólne ramy prawne dotyczące korzystania z usług zaufania. Ich katalog przewiduje również projekt ustawy. Państwom członkowskim pozostawiono swobodę określania innych rodzajów usług zaufania oprócz tych, które figurują w zamkniętym wykazie usług zaufania. Mogą utrzymać lub wprowadzić przepisy krajowe, zgodne z prawem unijnym, odnoszące się do usług zaufania, o ile usługi te nie są w pełni zharmonizowane w drodze rozporządzenia (projekt ustawy przygotowywany w Polsce). Usługi zaufania spełniające wymogi rozporządzenia powinny podlegać swobodnemu obrotowi na rynku wewnętrznym. Nie narzucono rozwiązań technologicznych dla wprowadzanych usług zaufania.

[8] **Tamże**

Określono natomiast skutki prawne, które powinny być osiągalne za pomocą dowolnego środka technicznego, o ile spełnione zostaną wymogi rozporządzenia eIDAS.

Część z wymienionych powyżej usług zaufania było uregulowanych w Polsce od wielu lat, jak np. podpis elektroniczny, czy znaczniki czasu. Jednak nowe przepisy wprowadzają zmiany także w tych znanych wcześniej usługach i to bardzo znaczne. Zmiany dotyczą przede wszystkim instytucji podpisu elektronicznego, usługi znakowania czasem oraz innych usług (tzw. usługi nienazwane). Obecnie trwają pracę nad nową ustawą, której zadaniem jest wprowadzenie instytucji uregulowanych w rozporządzeniu elDAS do polskiego systemu prawnego. Dotyczy to zarówno usług znanych i uregulowanych w Polsce, jak i usług nieznanych takich: jak e-doręczenia, czy e-konserwacja, co będzie wymagać odrębnej ustawy.

**Rysunek 1. Nowe uregulowania usług zaufania wprowadzane przez eIDAS**




Źródło: Opracowanie własne

Usługi zaufania, zarówno zamknięte, jak i otwarte, będą bez wątpienia w szerokim zakresie wykorzystywane w obszarze ochrony zdrowia.

W projektowanej regulacji[9] określono nadzór nad dostawcami usług zaufania. Nadzór sprawowany jest przez Ministra właściwego do spraw informatyzacji i w odniesieniu do kwalifikowanych dostawców usług zaufania realizowany jest m.in. przez:

- dopuszczenie dostawcy usług zaufania do świadczenia kwalifikowanych usług zaufania przez przyznanie statusu kwalifikowanego dostawcy usług zaufania i statusu kwalifikowanych usług zaufania świadczonym przez niego usługom;
- weryfikację spełnienia przez kwalifikowanych dostawców usług zaufania wymogów określonych w eIDAS[10]; odebranie kwalifikowanemu dostawcy usług zaufania statusu kwalifikowanego lub statusu kwalifikowanego świadczonej przez niego usłudze zaufania;
- żądanie niezwłocznego unieważnienia kwalifikowanych certyfikatów przez kwalifikowanego dostawcę usług zaufania;
- weryfikację zgodności polityk świadczenia usług z przepisami o usługach zaufania;
- nakładanie przewidzianych ustawą kar pieniężnych;
- współpracę z innymi organami nadzoru w kraju i zagranicą, a także z Europejską Agencją Bezpieczeństwa Sieci i Informacji.

Organ nadzoru może podejmować działania w stosunku do niekwalifikowanego dostawcy usługi zaufania w przypadku, gdy niekwalifikowany dostawca usługi zaufania nie spełnia wymogów eIDAS - w szczególności w przypadku zagrożenia bezpieczeństwa lub utraty integralności świadczonej przez niego usługi, jeżeli może zostać zagrożony interes odbiorców usługi zaufania.

## Krajowa infrastruktura zaufania

Organ nadzoru zapewnia funkcjonowanie krajowej infrastruktury zaufania, na którą składają się:

- zaufana lista - zawierająca informacje dotyczące kwalifikowanych dostawców usług zaufania

[9] Art. 4. projektu ustawy o usługach zaufania oraz identyfikacji elektronicznej z 03.06.2016 r. - https://legislacja.rcl.gov.pl/projekt/12283556, art. 4

[10] W sposób określony w art. 20 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr. 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE

- narodowe centrum certyfikacji usług zaufania – m.in tworzenie i wydawanie kwalifikowanym dostawcom usług zaufania certyfikatów służących do weryfikacji zaawansowanych podpisów elektronicznych lub pieczęci elektronicznych, publikacja danych służących do weryfikacji podpisów elektronicznych i pieczęci elektronicznych, publikacja listy unieważnionych certyfikatów
- rejestr dostawców usług zaufania.

W celu zapewnienia porównywalnego poziomu bezpieczeństwa kwalifikowanych usług zaufania, wszystkie państwa członkowskie powinny stosować wspólne podstawowe wymogi dotyczące nadzoru. Wszystkie państwa członkowskie powinny przyjąć porównywalne procedury i powinny wymieniać się informacjami na temat swoich działań nadzorczych oraz najlepszymi praktykami stosowanymi w tej dziedzinie. Wszyscy dostawcy usług zaufania powinni podlegać wymogom rozporządzenia, w szczególności wymogom dotyczącym bezpieczeństwa i odpowiedzialności, aby zapewnić należytą staranność, przejrzystość i rozliczalność ich operacji i usług. Biorąc jednak pod uwagę rodzaj usług świadczonych przez dostawców usług zaufania, należy, w odniesieniu do tych wymogów, dokonać rozróżnienia między kwalifikowanymi i niekwalifikowanymi dostawcami usług zaufania.

Ustanowienie systemu nadzoru dla wszystkich dostawców usług zaufania powinno zapewnić jednakowe zasady dotyczące bezpieczeństwa i rozliczalności ich operacji i usług, przyczyniając się w ten sposób do ochrony użytkowników i do funkcjonowania rynku wewnętrznego.

Niekwalifikowani dostawcy usług zaufania powinni podlegać łagodnym i reaktywnym działaniom nadzorczym *ex post,* uzasadnionym przez charakter ich usług i operacji. Organ nadzoru nie powinien zatem mieć ogólnego obowiązku nadzorowania niekwalifikowanych dostawców usług. Organ nadzoru powinien podejmować działania wyłącznie wtedy, gdy został poinformowany (na przykład przez samego niekwalifikowanego dostawcę usług zaufania, przez inny organ nadzoru, w drodze zgłoszenia od użytkownika lub partnera handlowego lub na podstawie własnego dochodzenia), że niekwalifikowany dostawca usług zaufania nie spełnia wymogów niniejszego rozporządzenia.

Aby umożliwić efektywne zainicjowanie procedury, która powinna doprowadzić do umieszczenia kwalifikowanych dostawców usług zaufania i świadczonych przez nich

kwalifikowanych usług zaufania na zaufanych listach, należy dążyć do nawiązania wstępnych interakcji między potencjalnymi kwalifikowanymi dostawcami usług zaufania a właściwym organem nadzoru, w celu ułatwienia należytej staranności niezbędnej do świadczenia kwalifikowanych usług zaufania. Zaufane listy są podstawowym elementem procesu budowania zaufania wśród operatorów rynku, ponieważ wskazują kwalifikowany status dostawcy usługi podczas nadzoru.

Zaufanie do usług *online* i ich wygoda mają podstawowe znaczenie dla użytkowników, by mogli w pełni korzystać z zalet usług elektronicznych i świadomie na tych usługach polegać. W tym celu należy stworzyć unijny znak zaufania, aby oznaczać kwalifikowane usługi zaufania świadczone przez kwalifikowanych dostawców usług zaufania. Taki unijny znak zaufania dotyczący kwalifikowanych usług zaufania pozwoliłby na wyraźne odróżnienie kwalifikowanych usług zaufania od innych usług zaufania, przyczyniając się tym samym do przejrzystości na rynku. Używanie unijnego znaku zaufania przez kwalifikowanych dostawców usług zaufania powinno być dobrowolne i nie powinno prowadzić do jakiegokolwiek wymogu innego, niż wymogi przewidziane w niniejszym rozporządzeniu.

## Usługa podpisu elektronicznego

W literaturze przedmiotu wyróżnia się obecnie osiem rodzajów podpisów elektronicznych, w zależności od zastosowanych technik i/lub technologii ich wytworzenia, tj. podpis klawiaturowy, podpis e-mailowy, podpis manualny, własnoręczny podpis biometryczny, podpis hasłowy, podpis mobilny, podpis kryptograficzny oraz podpis biometryczny. Podpis klawiaturowy polega na wpisaniu za pomocą klawiatury komputera imienia i nazwiska danej osoby bezpośrednio pod treścią dokumentu, z możliwością ich edycji na dowolnym programie komputerowym. Za taki rodzaj podpisu uważa się również podpis e-mailowy. Podobnie zeskanowanie podpisu własnoręcznego zapisanego w postaci cyfrowej traktowany jest jako podpis klawiaturowy. Złożenie podpisu za pomocą pióra cyfrowego przenoszącego do pamięci komputera specyficzne dla użytkownika przestrzenne wzory ruchów ręki skutkuje powstaniem podpisu manualnego. Do tej kategorii zalicza się także własnoręczny podpis biometryczny. Wprowadzając jednorazowe hasło z tokenu lub zdrapki, wraz z wykorzystaniem identyfikatora do logowania się w systemie informatycznym, posługujemy się

podpisem hasłowym. Zamiast hasła z tokenu lub zdrapki istnieje możliwość wpisania osobistego kodu PIN łącznie z numerem karty elektronicznej[11].

Osobną kategorię omawianej tematyki wyznaczają konsekwencje prawne poszczególnych rodzajów podpisów elektronicznych. Podpisem elektronicznym o najsilniejszych skutkach prawnych (porównywanych do formy pisemnej) stanowi bezpieczny podpis elektroniczny weryfikowany za pomocą ważnego kwalifikowanego certyfikatu. Z drugiej strony, niektóre rodzaje podpisu elektronicznego nie pociągają za sobą żadnych skutków prawnych, a dokumenty nimi asygnowane nie spełniają rygoru oświadczenia woli, ponieważ bezsprzeczna i jednoznaczna identyfikacja osoby podpisującej się, a tym samym składającej oświadczenie woli, przez odbiorcę wykracza poza obiektywne możliwości. Przykładem jest podpisanie imieniem i nazwiskiem dokumentu przesyłanego elektronicznie za pomocą wiadomości email lub wiadomości tekstowej (sms), gdzie adresat dokumentu nie jest w stanie zweryfikować autentyczności nadawcy.

Podpis elektroniczny to pojęcie znane w polskim systemie ochrony zdrowia od wielu lat[12]. Podpis, chociaż nie masowo, ale jednak był również wykorzystywany w ochronie zdrowia. Wynikało to przede wszystkim z przepisów prawa, które w określonych sytuacjach, przede wszystkim przy prowadzeniu dokumentacji medycznej w postaci elektronicznej, nakładały obowiązek stosowania tego rodzaju podpisu często w jego wersji kwalifikowanej tzw. bezpiecznego podpisu weryfikowanego kwalifikowanym lub niekwalifikowanym certyfikatem. Zmieniała się jednak narracja przepisów. Przepisy starsze wskazywały na poszczególne etapy tworzenia dokumentacji medycznej i wymagały do niej określonego rodzaju podpisu. Np. do sporządzania dokumentacji medycznej nie określono rodzaju podpisu elektronicznego, ale do udostępniania dokumentacji medycznej przepisy wymagały bezpiecznego podpisu weryfikowanego kwalifikowanym certyfikatem.[13]

W nowszych regulacjach dotyczących dokumentacji medycznej[14] pozostawiono decyzję o tym, jakiego rodzaju podpis jest stosowany kierownikowi podmiotu prowadzącego dokumentację medyczną.

[11] Marucha-Jaworska M., Podpisy elektroniczne, biometria, identyfikacja elektroniczna. Elektroniczny obrót prawny w społeczeństwie cyfrowym. Wydawnictwo Lex, Warszawa 2015
[12] Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym. Dz.U. 2001 nr 130 poz. 1450
[13] Rozporządzenie Ministra Zdrowia z dnia 21 grudnia 2006 r. w sprawie rodzajów i zakresu dokumentacji medycznej w zakładach opieki zdrowotnej oraz sposobu jej przetwarzania Dz.U. 2006 nr 247 poz. 1819
[14] Rozporządzenie Ministra Zdrowia z dnia 21 grudnia 2010 r. w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania Dz.U. 2010 nr 252 poz. 1697

## Podpisywanie i uwierzytelnianie dokumentów

Bardzo pozytywną zmianą jest rozdzielenie pojęcia „podpisywania" od „uwierzytelniania". Dokumenty (podania) po prostu się podpisuje, a nie uwierzytelnia. Poniższy cytat wyjaśnia istotę procesu podpisywania oraz uwierzytelniania *„Dokument, który podpisuję zaawansowanym podpisem elektronicznym opatruję danymi, które w przyszłości pozwolą na potwierdzenie jego źródła pochodzenia (autentyczność) oraz w przyszłości pozwolą na potwierdzenie jego integralności. Natomiast ponieważ celem jest jego przekazanie innej osobie, pozostawienie jako dowód w sprawie to badanie integralności podpisanego dokumentu a także źródła jego pochodzenia będzie należało do osoby, która ma podjąć późniejsze czynności prawne na bazie tego dokumentu, innymi słowy ma zaufać temu dokumentowi. To właśnie proces, w którym musimy zaufać dokumentowi, proces realizowany przez stronę ufającą jest uwierzytelnianiem, którego składowymi jest weryfikacja certyfikatu, walidacja podpisu, identyfikacja osoby podpisującej na podstawie certyfikatu a także weryfikacja integralności. Uwierzytelnienie jest procesem wykonywanym przez stronę ufającą samodzielnie lub z wykorzystaniem zewnętrznych usług tj. weryfikacja, walidacja. Natomiast podpis elektroniczny umożliwia wykonanie przez stronę ufającą tego procesu dostarczając dane potwierdzające źródło pochodzenia i dane pozwalające na rozpoznanie zmian podpisanych danych*[15]*:".*

Podobna zmiana dotyczy podpisywania pełnomocnictw przez osoby udzielające pomocnictwa. Także wskazano, że w tym przypadku mamy do czynienia z podpisywaniem a nie z uwierzytelnieniem. Zachowano jednak to pojęcie w odniesieniu do uwierzytelniania treści dokumentu wystawionego przez osobę trzecią.[16] „Uwierzytelnianie" to proces elektroniczny, który umożliwia identyfikację elektroniczną osoby fizycznej lub prawnej, lub potwierdzenie pochodzenia oraz integralności weryfikowanych danych w postaci elektronicznej.[17]

[15]M.Tabor; Uwierzytelnienie eIDAS to nie jest składanie podpisu elektronicznego http://notariat.pl/wiadomosci-notariat/374-uwierzytelnianie-w-eidas-to-nie-jest-skladanie-podpisu-elektronicznego
[16] Art. 33 § 3a i art. 220 KPA oraz odpowiednio art. 138a § 5 i art. 306d § 3 ordynacji podatkowej
[17] Art. 3 ust. 5 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr. 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE

W ostatnim czasie wprowadzono nowe przepisy o dokumentacji medycznej[18] oraz nastąpiły zmiany w przepisach o systemie informacji w ochronie zdrowia. Ustawa o systemie informacji w ochronie zdrowia nałożyła na pracowników medycznych obowiązek[19] używania bezpiecznego podpisu elektronicznego weryfikowanego przy pomocy ważnego kwalifikowanego certyfikatu[20] lub podpisu potwierdzonego profilem zaufanym ePUAP[21] do podpisywania:

- elektronicznej dokumentacji medycznej;
- wniosku o dostęp do danych umożliwiających pobranie z SIM elektronicznej dokumentacji medycznej lub danych z tych dokumentów, w zakresie niezbędnym do wykonywania badań diagnostycznych, zapewnienia ciągłości leczenia oraz zaopatrzenia usługobiorców w produkty lecznicze, środki spożywcze specjalnego przeznaczenia żywieniowego i wyroby medyczne;
- wniosku o dostęp do danych przetwarzanych w SIM umożliwiających wymianę między usługodawcami danych zawartych w elektronicznej dokumentacji medycznej.

Stoi to w kolizji z przepisami nowego rozporządzeniem regulującego zasady tworzenia dokumentacji medycznej w postaci elektronicznej. Przewiduje się przy tworzeniu dokumentacji medycznej składanie podpisu elektronicznego weryfikowanego przy wykorzystaniu wewnętrznych mechanizmów systemu teleinformatycznego. Wydaje się, że to rozwiązanie jest bliższe idei eIDAS oraz jest przepisem wykonawczym dotyczącym ustawy o prawach pacjenta[22], w której zawarto podstawowe regulacje dotyczące dokumentacji medycznej.

Podpis cyfrowy nie istnieje bez dokumentu elektronicznego, co jest wynikiem technologii jego tworzenia. W związku z tym niezwykle ważna jest definicja dokumentu elektronicznego. W rozporządzeniu eIDAS zdefiniowano dokument elektroniczny jako każdą treść przechowywaną w postaci elektronicznej, w szczególności tekst lub nagranie dźwiękowe,

[18] Rozporządzenie Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania Dz.U. 2006 nr 247 poz. 1819
[19] Art.17.3 Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia Dz.U. 2011 nr 113 poz. 657
[20] W rozumieniu ustawy z dnia 18 września 2001 r. o podpisie elektronicznym
[21] W rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne
[22] Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta Dz.U. 2009 nr 52 poz. 417 – rozdział 7

wizualne lub audiowizualne[23]; W związku z takim zdefiniowaniem dokumentu w ochronie zdrowia, dokumentami będą zarówno dokumenty dźwiękowe jak i dokumenty z diagnostyki obrazowej. Nie ma wymogu zapisania dokumentu na nośniku danych. Nie ma więc przeszkód w umieszczaniu dokumentów medycznych na wirtualnych nośnikach danych w chmurach obliczeniowych.

Nie można kwestionować skutku prawnego dokumentu elektronicznego, ani jego dopuszczalność jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że dokument ten ma postać elektroniczną[24].

## Zmiany dotyczące podpisu elektronicznego wprowadzone przez eIDAS

Wprowadzono nową definicję podpisu elektronicznego - *Podpis elektroniczny oznacza dane w postaci elektronicznej, które są dołączone lub logicznie powiązane z innymi danymi w postaci elektronicznej i które użyte są przez podpisującego jako podpis.*

Przewiduje się wprowadzenie w życie podpisu elektronicznego, zaawansowanego podpisu elektronicznego oraz kwalifikowanego podpisu elektronicznego.

Zastąpią dotychczas funkcjonujące: podpis elektroniczny, bezpieczny podpis elektroniczny oraz bezpieczny podpis elektroniczny weryfikowany za pomocą certyfikatu kwalifikowanego[25]. Zmiany znaczeniowe powodują konieczność dostosowania przepisów dotyczących pojęcia „bezpieczny podpis elektroniczny weryfikowany przy pomocy ważnego kwalifikowanego certyfikatu" równoważnym znaczeniowo pojęciem „kwalifikowany podpis elektroniczny". W projekcie ustawy zastępuje się „bezpieczny podpis elektroniczny" pojęciem „kwalifikowany podpis elektroniczny", jako najbliższy podpisowi kwalifikowanemu, lecz nie równoważnym znaczeniowo. Oznacza zaawansowany podpis elektroniczny, który jest

[23] Art. 3 ust. 35 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr. 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE
[24] Art. 46 rozporządzenia 12 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr. 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE
[25] Art.134 projektu ustawy o usługach zaufania oraz identyfikacji elektronicznej (projekt 3.06.2016)

składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego[26].

Zaawansowany podpis elektroniczny w znaczeniu eIDAS nie musi być składany za pomocą tzw. bezpiecznych urządzeń służących do składania podpisu elektronicznego. Określono następujące wymogi dla zaawansowanych podpisów elektronicznych:

- jest unikalnie przyporządkowany podpisującemu;
- umożliwia ustalenie tożsamości podpisującego;
- jest składany przy użyciu danych służących do składania podpisu elektronicznego, których podpisujący może, z dużą dozą pewności, użyć pod wyłączną swoją kontrolą; oraz
- jest powiązany z danymi podpisanymi w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna.

Innym rodzajem podpisu elektronicznego jest podpis elektroniczny potwierdzony profilem zaufanym ePUAP. Zgodnie z definicją podpis elektroniczny potwierdzony profilem zaufanym ePUAP[27] to podpis złożony przez użytkownika konta ePUAP, do którego zostały dołączone informacje identyfikujące zawarte w profilu zaufanym ePUAP, a także:

- jednoznacznie wskazujący profil zaufany ePUAP osoby, która wykonała podpis,
- zawierający czas wykonania podpisu,
- jednoznacznie identyfikujący konto ePUAP osoby, która wykonała podpis,
- autoryzowany przez użytkownika konta ePUAP,
- opatrzony i chroniony pieczęcią elektroniczną wykorzystywaną w ePUAP w celu zapewnienia integralności i autentyczności wykonania operacji przez system ePUAP.

Dane w postaci elektronicznej opatrzone podpisem elektronicznym potwierdzonym profilem zaufanym ePUAP są równoważne pod względem skutków prawnych dokumentowi opatrzonemu podpisem własnoręcznym, chyba że przepisy odrębne stanowią inaczej. Nie

[26] Art. 3 pkt. 12 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr. 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE

[27] W art. 3 pkt 15 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r. poz. 1114)

można odmówić ważności i skuteczności podpisowi elektronicznemu potwierdzonemu profilem zaufanym ePUAP tylko na tej podstawie, że istnieje w postaci elektronicznej lub zmianie uległy dane inne niż służące do potwierdzenia profilu zaufanego. Podpis wywołuje skutki prawne, jeżeli został utworzony lub złożony w okresie ważności tego profilu[28]. Podpis potwierdzony profilem zaufanym ePUAP nie jest zaawansowanym podpisem elektronicznym[29].

Ponadto, dostosowując przepisy do elDAS w celu zapewnienia integralności i autentyczności wykonania operacji przez system ePUAP oraz dołączenia podpisu elektronicznego potwierdzonego profilem zaufanym ePUAP wskazano, że nie używa się już „podpisu systemowego ePUAP", tylko zdefiniowanej w elDAS pieczęci elektronicznej.

W państwach członkowskich UE używa się obecnie różnych formatów zaawansowanych podpisów elektronicznych do elektronicznego podpisywania dokumentów elektronicznych. Państwa członkowskie powinny zapewnić możliwość obsługi pod względem technicznym co najmniej kilku formatów zaawansowanego podpisu elektronicznego przy odbiorze dokumentów podpisanych elektronicznie. Jest to tzw. zasada niedyskryminacji usług kwalifikowanych. W jej rezultacie kwalifikowany podpis elektroniczny, oparty na kwalifikowanym certyfikacie wydanym w jednym państwie członkowskim, jest uznawany za kwalifikowany podpis elektroniczny we wszystkich pozostałych państwach członkowskich[30].

Podobna konstrukcja została przyjęta w odniesieniu do pieczęci elektronicznej[31]. Kwalifikowana pieczęć elektroniczna, oparta na kwalifikowanym certyfikacie wydanym w jednym państwie członkowskim, jest uznawana za kwalifikowaną pieczęć elektroniczną we wszystkich pozostałych państwach członkowskich.

## Składanie podpisu elektronicznego na odległość

[28] Art. 20b ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r. poz. 1114)
[29] Uzasadnienie projektu ustawy o usługach zaufania oraz identyfikacji elektronicznej
[30] Art. 25 ust. 3 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr. 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE
[31] Art. 35 ust. 3 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr. 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE

Coraz powszechniejsze jest składanie podpisu elektronicznego na odległość. W takim przypadku środowiskiem składania podpisu elektronicznego zarządza dostawca usług zaufania w imieniu podpisującego. Dostawcy usługi składania podpisu elektronicznego na odległość powinni stosować szczególne procedury zarządzania i szczególne administracyjne procedury bezpieczeństwa, używać wiarygodnych systemów i produktów, w tym bezpiecznych kanałów komunikacji elektronicznej, aby zagwarantować niezawodność środowiska składania podpisu elektronicznego oraz korzystanie z tego środowiska pod wyłączną kontrolą podpisującego. W przypadku kwalifikowanego podpisu elektronicznego składanego za pomocą urządzenia do składania podpisu elektronicznego na odległość, należy stosować wymogi mające zastosowanie do kwalifikowanych dostawców usług zaufania, określone w rozporządzeniu eIDAS. Podpisującemu należy umożliwić korzystanie z kwalifikowanych urządzeń do składania podpisu elektronicznego, aby miał wyłączną kontrolę nad używaniem swoich danych służących do składania podpisu elektronicznego i aby urządzenie użytkowane spełniało wymogi dotyczące kwalifikowanego podpisu elektronicznego.

Przyjęto zasadę, że nie należy kwestionować skutku prawnego podpisu elektronicznego z tego powodu, że podpis ten ma postać elektroniczną lub że nie spełnia wszystkich wymogów kwalifikowanego podpisu elektronicznego. W prawie krajowym należy zdefiniować skutek prawny podpisów elektronicznych, zgodnie z którymi kwalifikowany podpis elektroniczny powinien mieć skutek prawny równoważny podpisowi własnoręcznemu.

Transgraniczna interoperacyjność i transgraniczne uznawanie kwalifikowanych certyfikatów stanowią warunek wstępny transgranicznego uznawania kwalifikowanych podpisów elektronicznych. Kwalifikowane certyfikaty nie powinny podlegać żadnym obowiązkowym wymogom oprócz tych zawartych w rozporządzaniu. Dopuszcza się jednak na szczeblu krajowym zawieranie w kwalifikowanych certyfikatach szczególnych atrybutów, takich jak unikalne identyfikatory, pod warunkiem, że takie szczególne atrybuty nie utrudniają transgranicznej interoperacyjności i transgranicznego uznawania kwalifikowanych certyfikatów i podpisów elektronicznych.

Certyfikacja bezpieczeństwa informatycznego, w tym urządzeń do składania podpisu elektronicznego, zostaje oparta na normach międzynarodowych, takich jak ISO 15408.

Innowacyjne rozwiązania i usługi, takie jak mobilny podpis i podpisywanie w chmurze, polegają na technicznych i organizacyjnych rozwiązaniach, jakimi są kwalifikowane urządzenia do składania podpisu elektronicznego, w odniesieniu do których mogą jeszcze nie być dostępne normy bezpieczeństwa lub pierwsza certyfikacja bezpieczeństwa informatycznego jeszcze trwa. Poziom bezpieczeństwa takich kwalifikowanych urządzeń do składania podpisu elektronicznego można by poddawać ocenie przy użyciu alternatywnych procedur tylko w przypadku, gdy takie normy bezpieczeństwa nie są dostępne lub gdy pierwsza certyfikacja bezpieczeństwa informatycznego jeszcze trwa. Procedury te powinny być porównywalne z normami certyfikacji bezpieczeństwa informatycznego w zakresie, w jakim ich poziomy bezpieczeństwa są równoważne. Procedury te mogłaby ułatwić wzajemna ocena.

## *Streszczenie*

W artykule omówiono ideę otwartych i zamkniętych usług zaufania oraz ich rodzaje. Przedstawiono koncepcję krajowej infrastruktury zaufania oraz narodowego centrum certyfikacji usług zaufania. Rozporządzenie eIDAS, między innymi, wprowadza zmiany w istniejących usługach jak np. podpis elektroniczny, jak również wprowadza nowe usługi jak pieczęć elektroniczna, uwierzytelnienie witryn internetowych oraz konserwacja elektronicznych podpisów, pieczęci i certyfikatów.

**Kontynuacja artykułu oraz wykaz piśmiennictwa znajdują się w części drugiej niniejszego opracowania.**